References to reputation risk have been removed from this booklet as of March 20, 2025. Removal of reputation risk references is identified by a strikethrough. Refer to OCC Bulletin 2025-4.

Internal Control

OTS requires all savings associations, their affiliates, and subsidiaries to establish and maintain adequate systems of internal control. Financial institutions must have a process in place to identify, monitor, and control risk. Audits by public accountants and examinations by all the banking agencies place a great emphasis on evaluating the appropriateness of the processes in place.

In this section of the Handbook, we do the following:

- Define internal control.
- Describe regulatory concerns.
- Discuss directorate and auditor responsibilities, including enterprise risk management.
- Present components of internal control.
- Provide guidance on assessing internal control risk.
- Discuss limitations of internal control.
- Explain how to consider internal control in planning and performing an examination.

LINKS

Program

Appendix A

Definition of Internal Control

The Auditing Standards Board (ASB) definition of internal control is in Statement of Auditing Standard (SAS) No. 78 (AU Section 319), *Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS 55*. The definition incorporates the common critical elements of internal control systems in the Committee of Sponsoring Organizations of the Treadway Commission (COSO) report, Internal Control – Integrated Framework, issued in 1992.

The COSO framework is the U.S. standard on internal control. COSO and SAS 78 define internal control "as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of the following objectives:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.

- Compliance with applicable laws and regulations."

The COSO model serves as the basis for the internal control assessment and reporting requirements for depository institutions presented in Section 112 of the FDICIA. This model is also broadly applicable to public companies in complying with Section 404 of the Sarbanes-Oxley Act. We discuss the Section 404 requirements later in this Handbook Section.

An effective internal control system better ensures the following important attributes:

- Safe and sound operations.
- The integrity of records, financial statements, and managerial reporting.
- Compliance with laws and regulations, and supervisory requirements.
- Decreased risk of unexpected losses.
- ~~Decreased risk of damage to the association's reputation.~~
- Adherence to internal policies and procedures.
- Efficient operations and long-term profitability targets.

A system of strong internal control is the backbone of an association's management program. Strong internal controls help an association meet goals and objectives, and maintain successful, healthy operations. Conversely, a lack of reliable records and accurate financial information may cause an association to fail. An effective internal control system integrated into the organization's overall risk management strategy serves the best interest of the shareholders, board of directors, management, and regulators.

Regulatory Concerns

Regulators place high importance on internal control systems in light of past corporate scandals and financial institution failures. Some institutions failed primarily because they did not detect insider fraud or abuse due to deficient or nonexistent systems of internal control. The types of control breakdowns typically seen in problem and failed institutions can be grouped into five categories:

- Lack of adequate management oversight and accountability, and failure to develop a strong control culture within the institution.
- Inadequate recognition and assessment of the risk of certain banking activities, whether on- or off-balance sheet.
- The absence or failure of key control structures and activities, such as segregation of duties, approvals, verifications, reconciliations, and review of operating performance.

- Inadequate communication of information between levels of management within the institution, especially in the upward communication of problems.

- Inadequate or ineffective audit programs and monitoring activities.

The Federal Deposit Insurance Corporation Improvement Act (FDICIA) of 1991 required the banking agencies to establish certain safety and soundness guidelines. Appendix A of 12 CFR Part 570, Interagency Guidelines Establishing Standards for Safety and Soundness, includes a section on operational and managerial standards. Under these standards, OTS requires management and the board of directors to implement and support effective internal controls appropriate to the size of the savings association, and the nature, scope, and risk of its activities.

Congress enacted the Sarbanes-Oxley Act of 2002 (SOX) to address failures in internal control, particularly over financial reporting. This law created a broad new oversight regime for auditors of public companies while prescribing steps to address specific failures and codifying the responsibilities of senior executive officers, directors, lawyers, and accountants. See Examination Handbook Section 310, Appendix A, for applicability of SOX requirements to financial institutions.

SOX created the Public Company Accounting Oversight Board (PCAOB), a private sector, nonprofit corporation, to oversee the auditors of public companies in order to protect the interests of investors and further the public interest in preparation of informative, fair, and independent audit reports.

Sarbanes-Oxley Requirements

Section 404 of SOX aims to strengthen the internal controls that underpin the accuracy and reliability of a company's published financial information. SOX includes a number of provisions designed to improve the corporate governance, financial disclosures and auditing relationships of public companies, including public banking organizations. Banking organizations are directly subject to SOX if they have a class of securities registered or they are required to file reports under the Securities Exchange Act of 1934.

Section 36 of the Federal Deposit Insurance Act (FDI Act) and Part 363 of the FDIC's regulations reflect SOX provisions and impose annual audit and reporting requirements on insured depository institution's with $500 million or more in total assets. Part 363 reporting requirements clarify what must be included in a Part 363 Annual Report for:

- Institutions with $500 million or more but less than $1 billion in total assets.

- Institutions with $1 billion or more in total assets.

- Other requirements applicable to all institutions subject to Part 363.

With certain exceptions, the Part 363 annual reporting requirements may be satisfied by an institution's holding company if services and functions comparable to those required of the institution are provided at the holding company level. We encourage the management, board of directors, and audit committee

of each institution subject to Part 363 and independent public accountants that provide audit and attestation services to institutions subject to Part 363 to read and become familiar with the Part 363 regulatory text, the Guidelines and Interpretations in Appendix A, and the Illustrative Management Reports in Appendix B to obtain a complete understanding of the compliance requirements of Part 363.

Nonpublic savings associations with less than $500 million in total assets are not subject to SOX or Part 363 of the FDIC's regulations.

DIRECTORATE RESPONSIBILITIES

The board of directors has the primary responsibility of establishing and maintaining an adequate and effective system of internal control. An effective board generally has members who have financial or banking experience and an obligation to stay current with innovations in corporate governance. See discussion of the BOD's responsibilities in Examination Handbook Section 310, Oversight by the Board of Directors.

The association's board must report to the FDIC and the OTS on internal control over financial reporting and compliance with certain laws and regulations, as well as file annual audited statements under Section 112 of FDICIA.

The board is also responsible for approving and periodically reviewing the overall business strategy and significant policies of the association, and understanding the major risks the association takes. The board should set acceptable levels for these risks, and ensure that senior management takes the required steps to identify, measure, and monitor these risks in order to mitigate them to acceptable levels. To remain effective in the dynamic and ever broadening environment that associations operate in, the board of directors should periodically review the system of internal control and ensure management regularly assesses and updates it.

The board and senior management must establish a strong culture of compliance at the top of the association, oversee anti-fraud programs at the association, and set a proper ethical tone for governing the conduct of business. Staff members at all levels must demonstrate successful completion of an ethics program.

Enterprise Risk Management

COSO released *Enterprise Risk Management – Integrated Framework* in September 2004. Enterprise risk management expands on internal control to form a more robust framework to effectively identify, assess, and manage risk. Enterprise risk management is interrelated with corporate governance by providing information to the board of directors on the most significant risks and how the association is managing those risks.

Enterprise risk management reflects certain fundamental concepts. It is:

- A process – ongoing and flowing throughout an entity.

- Effected by people at every level of an organization.
- Applied in a strategy setting.
- Applied across the savings association, at every level and unit, and includes taking an entity-level portfolio view of risks.
- Designed to identify events potentially affecting the association and manage risk within the board's risk appetite.
- Able to provide management and the board reasonable assurance that the association is managing its risk.
- Geared to the achievement of objectives in one or more separate but overlapping categories. That is, a particular objective can fall into more than one category – strategic, operations, reporting, and compliance.

The intent of the *Enterprise Risk Management – Integrated Framework* is not to replace the internal control framework, but rather to incorporate the internal control framework within it. Savings associations may decide to look to this enterprise risk management framework both to satisfy their internal control needs and to move toward a more robust risk management process.

An integral part of effective enterprise risk management is an enterprise-wide program that looks at how activities in one area of the association may affect the legal ~~and reputational~~ risks of other business lines and across the association as a whole. Enterprise risk management should consider how compliance with laws, regulations, and internal policies, procedures, and controls should be enhanced or changed. This approach is in marked contrast to the silo approach, which considers the legal ~~and reputational~~ risks of activities or business lines in isolation without considering how those risks interrelate and affect other business lines.

Audit Committee

The audit committee oversees internal control and the external and internal audit functions of an association. An active board or audit committee independent from management sets the association's control consciousness. The following parameters determine the effectiveness of an audit committee:

- The extent of its involvement in and its scrutiny of the association's activities.
- The ability to take appropriate actions.
- The degree to which the board or audit committee asks difficult questions and pursues the answers with management.

For additional guidance on audit committee responsibilities, see Handbook Sections 350, External Audit, and 355, Internal Audit.

AUDITOR RESPONSIBILITIES

Internal Audits

Both the internal and external auditors play key roles in monitoring the internal control systems. Each association should have an internal audit function that is appropriate to its size, and the nature and scope of its activities. The internal auditor is typically very involved in the ongoing review and assessment of an association's internal control. The board of directors should assign responsibility for the internal audit function to a member of management who has no operating responsibilities, and who is accountable for audit plans, programs, and reports. When properly structured and conducted, internal audits provide directors and senior management with vital information about any weaknesses in the system of internal control allowing management to take prompt, remedial action. Through directed reviews of the internal control systems and as part of the regular audit program, the internal auditor can be the first line of defense against a deficient control system. See Examination Handbook Section 355.

External Audits

Established policies and practices look to the external auditor to play a significant and vital role in an association's internal control systems. In this role, the external auditor performs procedures to attest to management's assertion that the internal control over financial reporting is functioning effectively when so engaged by the association (either because it is required by SOX or FDICIA, or voluntarily). The external auditor may consider the work done by the internal auditor as part of the auditing procedures.

Information Technology

SAS No. 94 (integrated in AU Section 319), *The Effect of Information Technology on the Auditor's Consideration of Internal Control*, which amends SAS No. 55, *Consideration of Internal Audit in a Financial Statement Audit*, provides guidance to external auditors about the effect of information technology on internal control. SAS 94 also establishes that an external auditor should obtain an understanding of internal control sufficient to plan the audit and determine the nature, timing, and extent of tests to perform, including assessment of control risk. This pronouncement places significant responsibility on the external auditor to look at internal control. The external auditor may not extensively review controls over all areas of the association, and may use different levels of testing depending on the risk of a specific area.

Communication of Internal Control Matters

SAS 112, *Communicating Internal Control Related Matters Identified in an Audit*, supersedes SAS 60 and is effective for audits of financial statements of nonpublic companies. In particular, SAS 112:

- Defines the term *significant deficiency,* (which replaces the SAS 60 term reportable condition) as a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with

GAAP such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is *more than inconsequential* will not be prevented or detected.

— A misstatement is inconsequential if a reasonable person would conclude, after considering the possibility of further undetected misstatements, that the misstatement, either individually or when aggregated with other misstatements, would clearly be immaterial to the financial statements. If a reasonable person would not reach such a conclusion regarding a particular misstatement, that misstatement is more than inconsequential.

- Revises the definition of *material weakness* as a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected.

- Provides guidance on evaluating the severity of control deficiencies identified in an audit of financial statements. SAS 112 states that a *control deficiency* exists when the design or operation of a control does not allow management or employees in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

- Requires the auditor to communicate, in writing, to management and those charged with governance, significant deficiencies and material weaknesses identified in an audit.

SAS No.115, Communicating Internal Control Related Matters Identified in an Audit, was issued in October 2008 and supersedes SAS No. 112. SAS No. 115 is effective for audits of financial statements of nonpublic companies for periods ending on or after December 15, 2009. Earlier implementation is permitted. SAS 115 was issued to eliminate differences within the AICPA's Audit and Attest Standards resulting from the issuance of Statement on Standards for Attestation Engagements (SSAE) No. 15, An Examination of an Entity's Internal Control Over Financial Reporting That Is Integrated With an Audit of Its Financial Statements. SSAE No. 15 was issued October 2008 and is effective for integrated audit periods ending on or after December 15, 2008. SSAE No.15 establishes standards and provides guidance to practitioners performing an examination of nonissuer's internal control over financial reporting to the context of an integrated audit. SSAE No. 15 aligns the definitions of the various kinds of deficiencies in internal control and the related guidance for evaluating such deficiencies with the definitions and guidance in Public Company Accounting Oversight Auditing Standards No. 5, An Audit of Internal Control That Is Integrated with an Audit of Financial Statements. SAS No.115, in turn, aligns the definitions and related guidance for evaluating deficiencies in internal control with the definitions and guidance in SSAE 15. In particular, SAS No.115 retains the core standards included in SAS No. 112 but contains the following revised definitions of the terms material weakness and significant deficiency:

- A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.

- A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

SAS No. 115 revises the list of deficiencies in internal control that are indicators of material weakness to consist of:

- Identification of fraud, whether or not material, on the part of senior management.

- Restatement of previously issued financial statements to reflect the correction of a material misstatement due to error or fraud.

- Identification by the auditor of a material misstatement of the financial statements under audit in circumstances that indicate that the misstatement would not have been detected by the entity's internal control.

- Ineffective oversight of the entity's financial reporting and internal control by those charged with governance.

SAS No. 115 no longer includes a list of deficiencies that were included in SAS No. 112 that ordinarily would be considered at least significant deficiencies. It also provides a revised illustrative written communication to management and those charged with governance of material weaknesses and significant deficiencies.

As mentioned earlier, SSAE No. 15 establishes standards and provides guidance to practitioners performing an examination of a nonissuer's internal control over financial reporting (internal control) in the context of an integrated audit (an audit of an entity's financial statements and an examination of its internal control). SSAE No. 15 supersedes AT section 501, *Reporting on an Entity's Internal Control Over Financial Reporting*. And converges the standards practitioners use for reporting on a nonissuer's internal control with Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 5, *An Audit of Internal Control That Is Integrated with an Audit of Financial Statements*- the long standing guidance followed by auditors of institutions subject to reporting requirement for internal control over financial reporting under FDICIA. SSAE is effective for integrated audits for periods ending on or after December 15, 2008.

SSAE No. 15 essentially mirrors the guidance for public companies subject to Section 404 of the Sarbanes-Oxley Act (SOX 404) and their auditors who follow PCAOB Auditing Standard No. 5. SSAE No. 15 establishes more extensive testing and documentation requirements than was previously required under the old AT 501. FDICIA engagements for nonpublic institutions, as well as institutions not yet subject to the provisions of SOX 404, which were governed by AT 501 are now governed by SSAE No. 15. Therefore, privately owned institutions over $1 billion in total assets now need to approach their documentation and testing of internal controls over financial reporting in a similar manner to that of a public company.

Audits of public companies are subject to PCAOB AS No. 5. The SEC is in agreement with PCAOB AS No. 5.

Audit of Internal Control Over Financial Reporting

PCAOB Auditing Standard No. 5, *An Audit of Internal Control Over Financial Reporting that is Integrated with an Audit of Financial Statements* establishes requirements and provides direction that applies when an auditor is engaged to perform an audit of management's assessment of the effectiveness of internal control over financial reporting that is integrated with an audit of the financial statements.

PCAOB Auditing Standard No. 5 defines *internal control over financial reporting* as:

> "A process designed by, or under the supervision of, the company's principal executive and principal financial officers, or persons performing similar functions, and effected by the company's board of directors, management, and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles (GAAP) and includes those policies and procedures that:
>
> - Pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company.
>
> - Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with GAAP, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company.
>
> - Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the association's assets that could have a material effect on the financial statements."

INTERNAL CONTROL COMPONENTS

SAS No. 78 provides guidance on the independent auditor's consideration of an entity's internal control in an audit of financial statements in accordance with generally accepted accounting standards. SAS No. 78 recognizes the definition and description of internal control contained in the COSO report, and provides an overview of the framework and evaluation tools needed for a strong system of internal control.

SAS No. 78 states that internal control consists of five interrelated components derived from the way management runs a business, and these components are integrated with the management process. The components are:

- Control environment

- Risk assessment

- Control activities
- Information and communication systems
- Monitoring.

The Control Environment

The effectiveness of internal controls rests with the people of the organization who create, administer, and monitor them. In varying degrees, internal control is the responsibility of everyone in the association. Integrity and ethical values are essential elements of a sound foundation for all other components of internal control. The commitment for effective control environment rests at the top. Reaching a conclusion about a financial institution's internal control environment involves a degree of subjectivity because of the intangible nature of measuring effectiveness.

Control Environment Assessment Process

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Draw conclusions as to the quality of risk management and assess the effectiveness of the control environment in the following areas:

Integrity and Ethical Values

Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical values are the products of the association's ethical and behavioral standards. How management communicates and reinforces these values in practice establishes the tone for the organization. Management should strive to remove or reduce incentives and temptations that might prompt employees to engage in dishonest, illegal, or unethical acts. Management must also communicate their values and behavioral standards to personnel through policy statements and codes of conduct.

Commitment to Competence

Competence is the knowledge and skills necessary to accomplish tasks that define the individual's job. Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.

Board of Directors or Audit Committee Participation

The association's board of directors or audit committee significantly influences an association's control consciousness. Attributes include the board or audit committee's independence from management, the experience and stature of its members, the extent of its involvement in and scrutiny of activities, the appropriateness of its actions, the degree to which difficult questions are raised and pursued with management, and its interaction with internal and external auditors.

Management's Philosophy and Operating Style

Management's approach to taking business risks and their attitude toward financial reporting (conservative versus aggressive) and information processing weigh heavily in the control environment. Consider the level of commitment by management and the board of directors to establish the necessary foundation on which to build an effective system of internal control. Management must have the will to make policies work; otherwise even the best-written policies on internal control would not be effective.

Organizational Structure

The association must have an organizational structure that supports its objectives. Management must plan, execute, control, and monitor association objectives. It must establish key areas of authority and responsibility and appropriate lines of reporting. The appropriateness of an entity's organizational structure depends, in part, on its size and the nature of its activities.

Assignment of Authority and Responsibility

This factor includes how the board and senior management assign authority and responsibility for operating activities and establish reporting relationships and authorization hierarchies. It also includes policies relating to the following areas:

- Appropriate business practices.
- Knowledge and experience of key personnel.
- Resources for carrying out duties.

Human Resource Policies and Practices

Human resource policies and practices relate to hiring, orientation, training, evaluating, counseling, promoting, compensating, and remedial actions. Human resource policies and practices send messages to employees regarding expected levels of performance, integrity, ethical behavior, and competence. Promotions driven by periodic performance appraisals demonstrate the association's commitment to the advancement of qualified personnel to higher levels of responsibility.

Risk Assessment

All entities, regardless of size, encounter risk in their organizations. The ability to identify and manage these risks will affect an entity's ability to survive in a competitive market. In order to assess risk, management must first set objectives to quantify the amount of risk they can prudently accept.

Risks relevant to financial reporting include external and internal events, and circumstances that may adversely affect an association's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements. Such risks can arise or change due to the following circumstances:

- Operating environment changes
- New personnel
- New or redesigned information systems
- Rapid growth
- New technology
- New business models, products, or activities
- Corporate restructurings
- New or expanded foreign operations
- New accounting pronouncements.

The Risk Assessment Process

Determine whether management has identified and analyzed the risks, and has methodologies in place to control them. Consider also the following areas in assessing the risk process:

- Prevalence of external and internal factors that could affect whether the association achieves strategic objectives.
- Effectiveness of systems used to manage and monitor the risks.
- Capacity of existing processes to react and respond to changing risk conditions.
- Level of competency, knowledge, and skills of personnel responsible for risk assessment.

Control Activities

Control activities are the policies, procedures, and practices established to help ensure that association personnel carry out board and management directives at every business level throughout the association. Control activities should assure accountability in the association's operations, financial reporting, and compliance areas. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, review of operating performance, security of assets, and segregation of duties.

The Control Activities Assessment Process

Assessment of control activities relevant to an examination includes the elements discussed below.

Performance Reviews

Management should establish policies and procedures to ensure control activities include reviews of actual performance versus budgets, forecasts, and prior period performance.

Management should conduct independent checks or verifications on function performance and reconciliation of balances.

Information Processing

There are two categories of controls for information systems:

- *General controls* apply to mainframe and end-user environments.

  Management should establish policies and procedures to ensure that general controls are commonly in place over the following areas:

  — Data center and network operations.

  — System software acquisition and maintenance.

  — Access security.

  — Application system acquisition, development, and maintenance.

- *Application controls* apply to the processing of individual applications.

  Management should establish controls to ensure valid, complete, properly authorized, and accurately processed transactions.

Information technology (IT) examiners review information processing controls in IT examinations.

Physical Controls

Management should establish safeguards and physical controls over the following activities:

- The physical security of assets, such as secured facilities.
- Access to books, and sensitive records and systems.
- Granting access to systems, applications, and databases.

- Periodic counting and comparison with amounts shown on control records.

Segregation of Duties

Management must assign different people the responsibility of authorizing transactions and recording transactions, and maintaining custody of assets. Management also should ensure that personnel adhere to vacation requirements and periodic rotation of duties for personnel in sensitive positions. This segregation of duties should reduce the opportunities to perpetrate and conceal errors, irregularities, or wrongdoing.

An independent third party should periodically review this area to ensure segregation of duties is effective.

Information and Communication Systems

Information and communication systems support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.

An information system consists of infrastructure (physical and hardware components), software, people, procedures, and data. Many information systems make extensive use of information technology.

Information systems produce reports containing operational, financial, and compliance-related information that make it possible to run and control the business. An association should have policies, procedures, and controls to ensure the confidentiality, integrity, and availability of its information.

To be effective, management must communicate information to the people who need it to carry out their responsibilities. Management must design ways to downstream messages from the top, as well as upstream significant information. There also needs to be effective communication with external parties, such as customers, suppliers, service providers, regulators, and shareholders.

Information and Communication Systems Assessment Process

An information system should provide sufficient detail to properly classify the transaction for financial reporting, and measure the transactions in a manner that permits recording the proper amounts in the financial statements in accordance with GAAP.

Communication involves an understanding of individual roles and responsibilities pertaining to internal control over financial reporting. Determine whether policy manuals, accounting and financial reporting manuals, and other memoranda effectively communicate internal control responsibilities.

Determine if management established systems to capture and impart pertinent and timely information in a form that enables staff to carry out their responsibilities. Also, determine whether the following safeguards exist:

- Accounting systems identify and record all valid transactions in the proper accounting period; ensure accountability for related assets, liabilities, equity, income, and expense; and present transactions and related disclosures in the financial statements.

- Management information systems identify and capture relevant internal and external information in a timely manner.

- Association-wide business continuity plans and disaster recovery plans for the association's information systems. For additional guidance, see Examination Handbook Section 341, Information Technology Risks and Controls, and CEO Memo No. 269, FFIEC IT Examination Handbook, Business Continuity Planning.

Monitoring

Monitoring is a process that assesses the quality of the internal control performance over time. It involves assessing the design and operation of controls on a timely basis and taking necessary corrective actions. COSO issued an exposure draft in June 2008 titled *Guidance on Monitoring Internal Control Systems.*

Management must build ongoing monitoring activities into the normal recurring activities of their association, and monitor the internal control system on an ongoing basis to ensure that the system continues to be relevant and addresses new risks. Monitoring of key risks should also be part of the association's daily activities. In many cases, the internal auditor is responsible for monitoring the entity's activities, including key risks, and regularly provides information about the functioning of internal control, including the design and operation.

The Monitoring Assessment Process

Determine who oversees and assesses the monitoring process. Review the type of monitoring or periodic evaluation of internal control that occurs. For example, is it by self-assessment, by independent audit, or a separate risk management group? Check whether systems ensure timely and accurate reporting of deficiencies and whether there are processes to ensure timely modification of policies and procedures, as needed. Determine whether internal control deficiencies are reported to the appropriate person, with all serious matters reported to top management and the board.

Integrated System of Internal Control

There is synergy and linkage among these five internal control components, forming an integrated system that reacts dynamically to changing conditions. The internal control system intertwines with the association's operating activities and exists for fundamental business reasons. Internal control is most effective when management builds controls into the association's infrastructure and the controls become a part of the essence of the association. "Built in" controls support quality and empowerment initiatives, avoid unnecessary costs, and enable quick response to changing conditions.

There is a direct relationship between the three categories of objectives listed in the COSO and SAS 78 definition of internal control and the components. The objectives are what an association strives to achieve, and the components represent what the association needs to achieve the objectives. All components are relevant to each objectives category. When looking at any one category – the

effectiveness and efficiency of operations, for instance – all five components must be present and functioning effectively to conclude that internal control over operations is effective.

After examining the components and their risk, draw an overall conclusion as to the adequacy of the association's system of internal control and, if appropriate, include the assessment in the report of examination. A system deemed inadequate is potentially in noncompliance with Appendix A of 12 CFR Part 570, Interagency Guidelines Establishing Standards for Safety and Soundness. OTS may notify an association with an inadequate risk assessment of the need to file a plan of compliance as the regulation provides. The plan would establish how the association will correct its internal control deficiencies.

LIMITATIONS OF INTERNAL CONTROL

When operating under the best of conditions, internal control provides only reasonable assurance to management and the board of directors that the association is achieving its objectives. Reasonable assurances do not imply that the internal control systems will never fail. Many factors, individually and collectively, serve to provide strength to the concept of reasonable assurance. However, because of inherent limitations, management has no guarantee that, for example, an uncontrollable event, a mistake, or improper reporting incident could never occur. Thus, it is possible for the best internal control system to fail. The limitations inherent to internal control are:

- Judgment
- Breakdowns in internal control
- Management override
- Collusion
- Fraud
- Cost versus benefits.

We discuss each of these limitations below.

Judgment

Human judgment can limit the effectiveness of internal controls. Management makes business decisions based on the information at hand and under time constraints. With hindsight, these decisions may produce less than desirable results.

Breakdowns in Internal Control

The best internal control system can experience any of the following breakdowns:

- Misunderstood instructions

- Careless employees
- Inadequate training
- Time limitations.

Management Override

Management override means management overrules prescribed policies or procedures for illegitimate purposes with the intent of personal gain or to enhance the presentation of financial statements. Override practices include deliberate misrepresentations to regulators, lawyers, accountants, and vendors.

Do not confuse management override with management intervention. Management intervention represents management's actions that depart from prescribed policies for legitimate purposes. At times, management intervention is necessary to deal with nonrecurring and nonstandard transactions or events, that otherwise might be handled inappropriately by the control system.

Collusion

When two or more individuals act in concert to perpetrate and conceal an action from detection, they can circumvent any system of internal control.

Fraud

Fraud is a broad legal concept, and involves intentional illegal acts that generally cause misstatement in the financial statements. Management bears the primary responsibility for detecting fraud. Internal control systems implementation is part of management's fiduciary responsibilities to prevent fraud and abuse by insiders. While the primary objective of an examination is the qualitative analysis of the association, fraud detection is certainly a goal when reviewing an association's internal control system. The opportunity to commit and conceal fraud exists when the association has assets susceptible to misappropriation and a lack of internal control to prevent and detect fraud.

An examination of internal controls with an eye to the weaknesses in any one of the five components of the system will identify the association's exposure to fraud. Next, you should look for symptoms suggesting that fraud is occurring or has occurred in those areas. For misappropriation of assets, fraud symptoms generally can be classified into the following categories:

- Accounting symptoms – unusual or suspicious items involving the organization's accounting records or related documents.
  - Source documents that have been manipulated.
    - Missing documents

- Alterations of documents
- Duplicate payments
- Stale items on association reconciliations
- Increased reconciling items.

— Journal entries where a fraudulent debit has been recorded.

- Entries without supporting documentation.
- Entries made by persons who do not normally make those entries.
- Entries made near the end of the period.

— Accounting ledgers not in agreement with related accounts:

- Ledger does not agree with underlying assets.
- Subsidiary ledger does not agree with the control account.

- Analytical symptoms – relationships, procedures, or events that do not make sense. Relationships may be symptoms if they are too unusual or too unrealistic to be believable. Events and transactions may be symptoms if they (1) happen at odd times or places; (2) are performed by or involve people who would not normally participate; (3) involve odd procedures, polices, or practices; or (4) are performed or occur too often or too rarely.

  — Unexplained shortages or adjustments in accounts.

  — Significant increases or decreases in account balances.

  — High numbers or amounts of past due accounts.

  — Suspense accounts with high or continuing balances.

  — Cash shortages or overages.

  — Excessive late charges.

  — Unreasonable expenses or reimbursements.

Problems concerning insiders at some associations have some commonalities. Potential red flags that could signal fraud include the following situations:

- Management that is hostile or uncooperative towards examiners.

- Significant insider transactions that the association improperly approves or fails to fully document.
- Basic internal control deficiencies, such as failure to separate functions or rotate duties.
- Poor or incomplete documentation.
- Financial accounting systems and reports are unreliable, underlying controls are deficient, or the reconciliation process is lacking.
- Repeated and significant Thrift Financial Report reporting errors.
- Continuing unsafe and unsound conditions.

You should be aware of the potential warning signs of fraud and the examination and audit procedures that you should employ when warranted. If you encounter any red flags, you should investigate the situation and consider whether to seek assistance from agency subject matter experts, (such as regional accountants, IT examiners, etc.). For more information, see Handbook Section 360, Fraud and Insider Abuse.

Costs versus Benefits

Management makes quantitative and qualitative estimates and judgments in evaluating the cost-benefit relationship of the association's internal control. The challenge is to find the right balance between the proper controls and the costs to design and implement internal controls. Excessive control is costly and counterproductive. Too few controls present undue risks.

Examination Considerations

The objective of examining the internal control of an association is to assess the extent management has established internal control procedures and programs to identify and mitigate the association's internal control risks. You should focus your efforts on the detection, exposure and correction of important weaknesses in the association's records, operating systems, and auditing procedures. Gather information through discussions with management and employees and observation of performance and procedures. You must apply common sense and technical knowledge to the specific situations of each association. You must consider the association's size, the number of employees, and the character of the association's operations. In planning the examination, be aware of the following situations that may suggest that there is a breach in the control system that warrants attention:

- Management does not implement effective procedures to correct internal deficiencies noted in audit reports or reports of examination.
- Management scales back or suspends the internal audit or risk management function.

- The internal auditor has an operational role in addition to audit responsibilities.

  For example, the internal auditor reports through operating management and not directly to the board of directors or a committee. Ideally, the internal audit function should be under the board of directors or the audit committee, and the internal auditor should report directly to them. The extent to which the internal auditor reports to management may warrant attention to ensure that such reporting does not impair the independence of the internal auditor.

- The association's external audit firm lacks depository institution audit experience, the auditors assigned have limited experience, or are geographically distant.

- Association management enters new areas of activity without first implementing proper controls, or engages in new activities without experienced staff and appropriate controls in place.

- Management fails to provide adequate reports to the board of directors.

- Management fails to report on the association's internal control over financial reporting and/or external auditors fail to attest to the accuracy of management's report.

- The association does not have proper controls in high-risk areas.

- The association often deviates from board-approved policies with exception documentation.

- The association fails to effectively segregate duties and responsibilities among employees.

- The association had a security breach that resulted in unauthorized access to or use of customer information.

In general, when beginning an examination, first review and evaluate the adequacy and effectiveness of the internal control system. If you discover areas where internal controls are inadequate, expand the scope of examination to determine whether there are any safety and soundness concerns.

Level I Procedures

Review the list of objectives in the Internal Control Program and follow the Level I Procedures to design the examination. These procedures are generally sufficient when an association has an effective internal audit or risk management function.

Although the five components of internal control provide a useful framework for you to review the effect of an entity's internal control in an examination, they do not reflect how the association considers and implements internal control. Therefore, you should consider the five internal control components in the context of the following criteria:

- Size of the association.

- Organization and ownership characteristics.
- Nature of the association's business.
- Diversity and complexity of the association's business.
- The association's information technology environment, including all methods of capturing, transmitting, processing, maintaining, and accessing information. See Examination Handbook Section 341 for additional guidance.
- Legal and regulatory requirements.

Management's Responses to Questionnaires

OTS sends the Internal Control Questionnaire and the Funds Transfer Questionnaire to the association as part of the PERK. Association management completes the questionnaires, which contain questions regarding the overall internal control system of the association. You should verify answers provided by management to ensure that the answers accurately reflect the association's activities and the adequacy of its control environment.

In both the Internal Control and Funds Transfer Questionnaires, there are certain "flagged" questions that are the suggested minimum verifications you should perform through inquiry, observation, or testing, particularly if the association lacks effective controls.

You should also review the general questionnaires that correlate to certain handbook sections as examiners assigned these areas complete them. Identify all critical internal control deficiencies. Discuss these deficiencies with management and encourage them to take appropriate corrective action.

Internal Audit Work Papers

Examine samples of work papers from internal audits, and include samples from outsourced functions or director's examinations. The samples should be sufficient to provide a basis to validate the scope and quality of the association's internal control system, and determine the amount of reliance, if any, you can place on the system.

Review also, whether the external auditor communicated any deficiencies, either orally or in writing, to management. If you determine that external audit work papers are necessary for your review, contact your field manager or the Regional Accountant before requesting external audit work papers, or other pertinent documents related to the external auditor's judgment about the association's internal control. See Handbook Section 350 for requesting external audit work papers, Appendices D and E.

Make requests for work papers specific to the areas of greatest interest. The request may include related planning documents and other pertinent information related to the internal control areas in question. If management or the internal auditor refuses to provide access to the work papers, contact the Regional Accountant or Legal division.

If the internal audit work papers review or the external auditor's communications with management on deficiencies raises concerns about internal audit effectiveness, discuss the issues with management, the board of directors, and the audit committee. If issues remain unresolved regarding external audit work, consult with the Regional Accountant.

Level II Procedures

Based on management's responses to questionnaires, or when an association does not have an effective system of internal audit, or when warranted based on examination findings, consider expanding the scope of the examination to include Level II procedures provided in the Internal Control Program. Also perform appropriate Level II procedures if the association outsources any significant activities and Level I procedures are insufficient to determine how the association controls the outsourced activity.

Issues that would require expanded procedures under Level II include:

- Concern about the competency or independence of internal auditors.
- No internal or external audit program is in place.
- Unexplained or unexpected changes occurring in the internal or external auditors or significant changes occurring in the audit program.
- Inadequate controls in key risk areas.
- Deficient audit work papers in key risk areas, or work papers that do not support audit conclusions.
- Rapid growth areas exist without adequate audit or internal control.
- Inappropriate actions by insiders to influence the findings and scope of audits.

After completion of Level II procedures, if significant concerns remain about the adequacy of internal control, consider expanding the scope of the review to include procedures under Level III of the Internal Control Program.

The following situations may warrant Level III procedures:

- Account records are significantly out of balance.
- Management is uncooperative or poorly manages the thrift.
- Management restricts access to records.
- Significant accounting, audit, or internal control deficiencies remain uncorrected from previous examinations or from one audit to the next.

- Internal auditors are unaware of, or unable to sufficiently explain, significant deficiencies.
- Management engages in activities that raise questions about its integrity.
- Repeated violations of law affect audit, internal control, or regulatory reports.
- Other situations that you believe warrant further investigation.

Consult with your EIC, field manager, or the Regional Accountant to determine which procedures you should perform. Where you determine that the association's internal control system is not adequate or effective for its specific risk profile, consult with your EIC, field manager, or Regional Accountant on appropriate corrective action.

OUTSOURCING RISKS

Associations rely increasingly on services provided by third parties to support a wide range of activities. Outsourcing, both to affiliated companies or third parties, may help manage costs, improve and expand services offered, and obtain expertise not internally available. At the same time, reduced operational control over outsourced activities may expose an association to additional risks.

Outsourcing involves some of the same operational risks that arise when an association performs a function internally. Such risks include the following:

- Threats to the availability of systems used to support customer transactions.
- The integrity or security of customer account information.
- The integrity of risk management information systems.

Under outsourcing arrangements, however, the risk management measures commonly used to address these risks, such as internal controls, are generally under the direct control of the service provider, rather than the association that bears the risk of financial loss~~, damage to its reputation,~~ or other adverse consequences.

OTS expects associations to ensure that controls over outsourced activities are equivalent to those that the association would implement if they conducted the activity internally. The association's board of directors and senior management should understand the key risks associated with the use of service providers. They should ensure that an appropriate oversight program is in place to monitor each service provider's controls, condition, and performance.

See discussions of outsourcing in Handbook Sections 341 Information Technology Risks and Controls, and 355, Internal Audit; Thrift Bulletin (TB) 81, Interagency Policy Statement on the Internal Audit Function and its Outsourcing; TB 82a, Third Party Arrangements; and the FFIEC IT Examination Handbook.

REFERENCES

United States Code (12 USC)

Federal Deposit Insurance Act

§ 1831	Contracts Between Depository Institutions and Persons Providing Goods, Products, or Services
§ 1831p-1	Standards for Safety and Soundness

Federal Deposit Insurance Corporation Improvement Act (FDICIA)

§ 112	Independent Annual Audits of Insured Depository Institutions

Code of Federal Regulations (12 CFR)

74 FR 35726	Final Rule; Annual Independent Audits and Reporting Requirements (July 29, 2009)
Part 363	Requirements For External Audits and Audit Committees
Part 364 Appendix A	Interagency Guidelines Establishing Standards for Safety and Soundness
Part 562	Regulatory Reporting Standards
Part 570	Appendix A, Interagency Guidelines Establishing Standards for Safety and Soundness

Sarbanes-Oxley Act of 2002

§ 404	Management's Report on Internal Control Over Financial Reporting

OTS References

CEO Memo 173	Filing of Section 906 SOX Certifications with OTS
CEO Memo 174	Statement by the Federal Reserve Board, the Comptroller of the Currency, and the Office of Thrift Supervision on Application of Recent Corporate Governance Initiatives to Non-Public Bank Organizations
CEO Memo 180	SEC's Final Rule Discussing Reports on Internal Control That May Satisfy Both SEC Requirements and FDIC Part 363 Requirements
CEO Memo 245	Directors' Guide to Management Reports

CEO Memo 269	Information Technology Handbook, Updated Business Continuity Planning Booklet
TB 81	Interagency Policy Statement on the Internal Audit Function and its Outsourcing
TB 82a	Third Party Arrangements
Transmittal 388	SEC Extends Date Regarding the Internal Controls Requirements Mandated by Section 404 of SOX
Transmittal 392	SEC Issued Final Rule on Amendments to Rules Regarding Management's Report on Internal Control Over Financial Reporting

Closely Related Examination Handbook Sections

341	Information Technology Risks and Controls
350	External Audit
355	Internal Audit

FFIEC IT Examination Handbook

AICPA Professional Standards

Statement on Auditing Standards (SAS) (U.S. Auditing Standards (AU))

No. 55	Consideration of Internal Control in Financial Statement Audit (AU 319)
No. 60	Communication of Internal Control Structure Related Matters Noted in an Audit (AU 325)
No. 78	Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS 55 (AU 319)
No. 91	Federal GAAP Hierarchy
No. 94	The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit (AU 319)
No. 112	Communicating Internal Control Related Matters Identified in an Audit

No. 115	Communicating Internal Control Related Matters Identified in an Audit (Supersedes SAS No. 112 and is effective for periods ending on or after December 15, 2009)
AU Section 319	Consideration of Internal Control in a Financial Statement Audit
AU Section 325	Communications About Control Deficiencies in an Audit of Financial Statements

Audit and Attest Standards

AT 501	Reporting on an Entity's Internal Control Over Financial Reporting
SSAE 15	An Examination of an Entity's Internal Control Over Financial Reporting that is Integrated with an Audit of its Financial Statements (Supersedes AT 501 and is effective for periods ending on or after December 15, 2008)

Public Company Accounting Oversight Board (PCAOB)

Auditing Standard No. 5, An Audit of Internal Control Over Financial Reporting that is Integrated with an Audit of Financial Statements